

RSA[®]Conference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN
ELEMENT

SESSION ID: EZCL-R01

Maturing Cyber-Risk Management Practices: Framework and Next Steps



Jack Freund, Ph.D.

Director, Risk Science

RiskLens

@jackfreund3

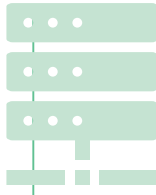
#RSAC

What does a mature risk management organization look like?

#RSAC



Appropriate policies and procedures are clearly defined and documented



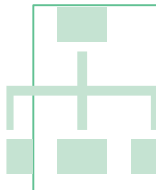
Cost-effective security technologies are providing their intended value



An effective education and awareness program exists



Personnel roles and responsibilities are properly defined and staffed



Board of directors are getting the information they need



A risk register is used to track and report the most important risks

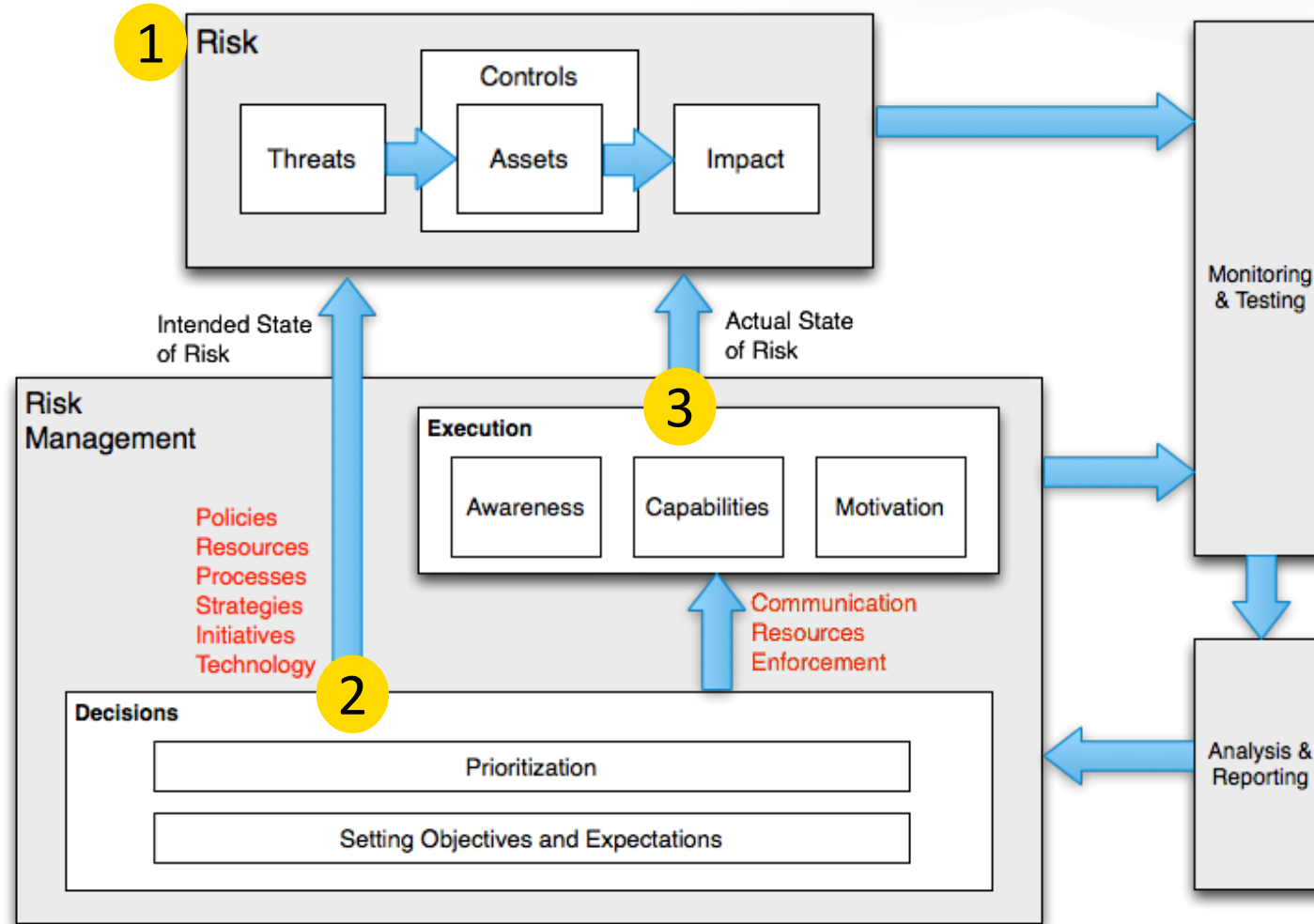


A clearly defined risk appetite actively drives decision-making

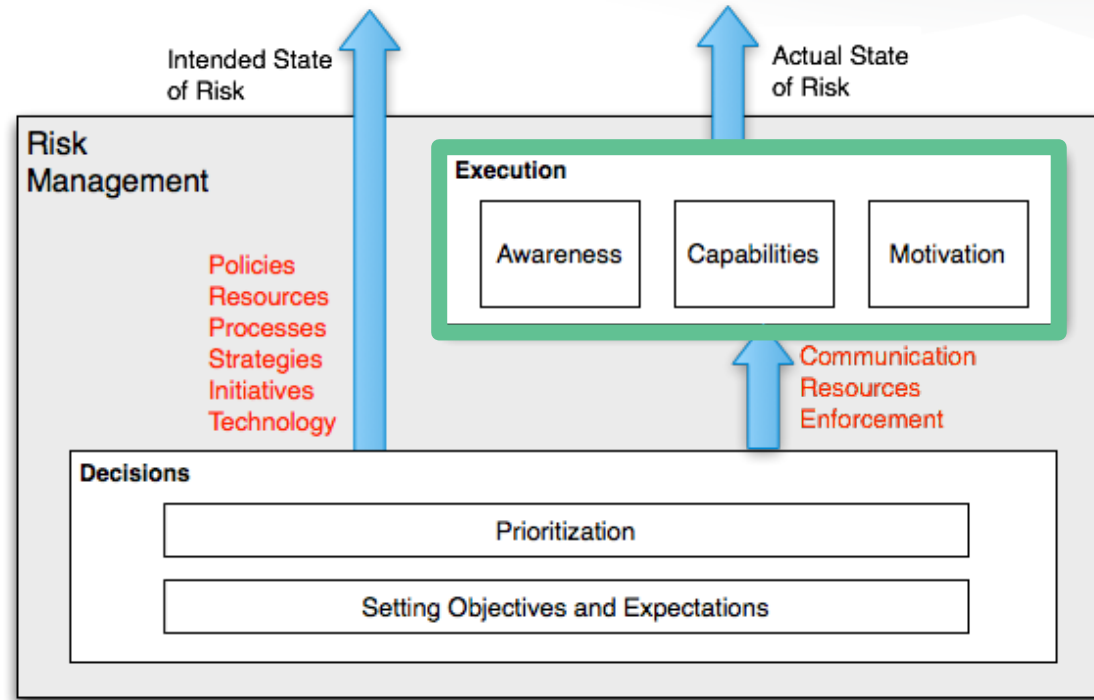


Meaningful metrics are leveraged to manage risk effectively

Risk Management Landscape



Execution



Awareness

The probability that personnel are aware of their risk management roles and responsibilities, and the specific expectations of organization leadership.

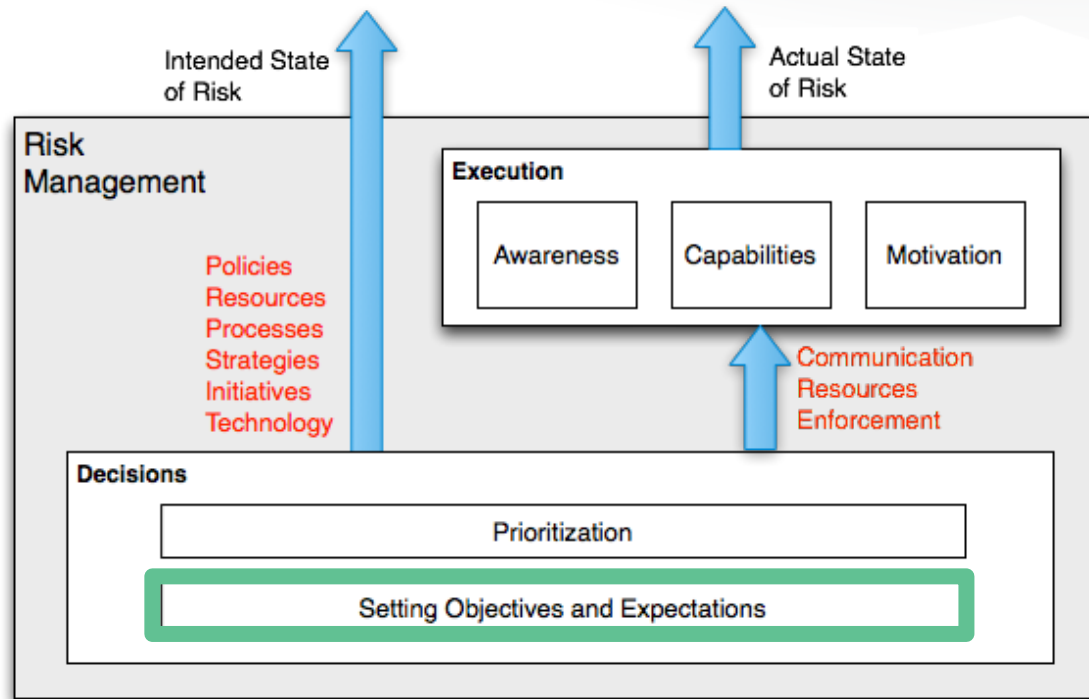
Capability

The probability that personnel have the necessary skills and resources to successfully execute their roles and responsibilities.

Motivation

The probability that personnel are appropriately incentivized to fulfill their risk management responsibilities

Objectives and Expectations



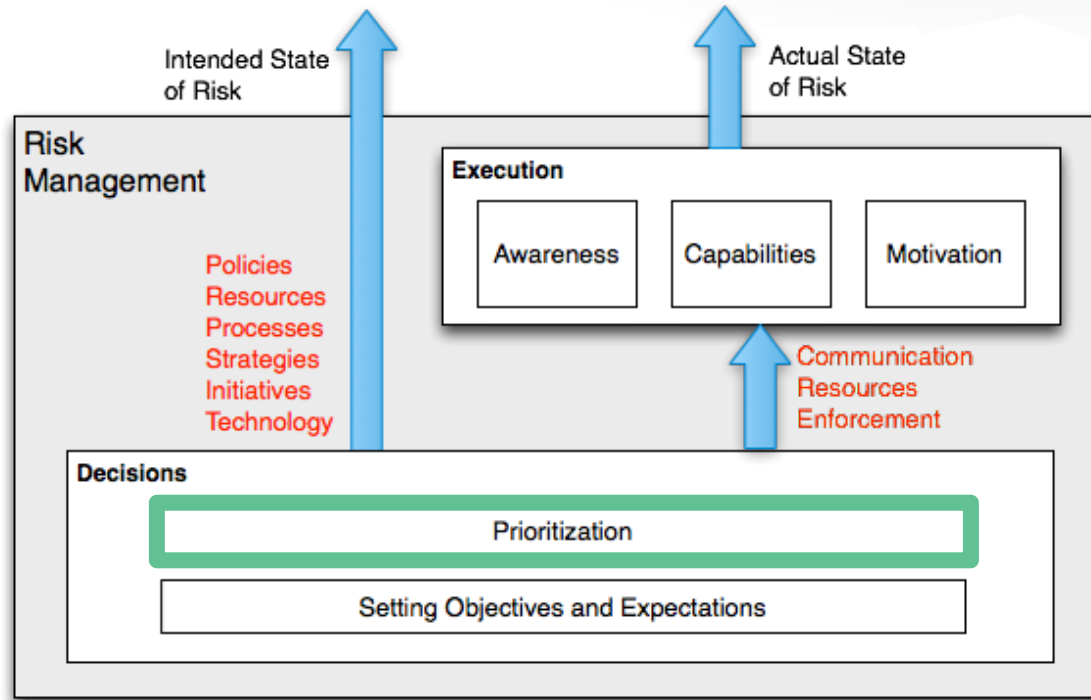
Compliance Requirements

The degree to which an organization is subject to meaningfully enforced external risk management expectations.

Prioritization

The probability that decision-makers are provided with the information needed to establish priorities and choose solutions, both at a strategic and operational level.

Prioritization

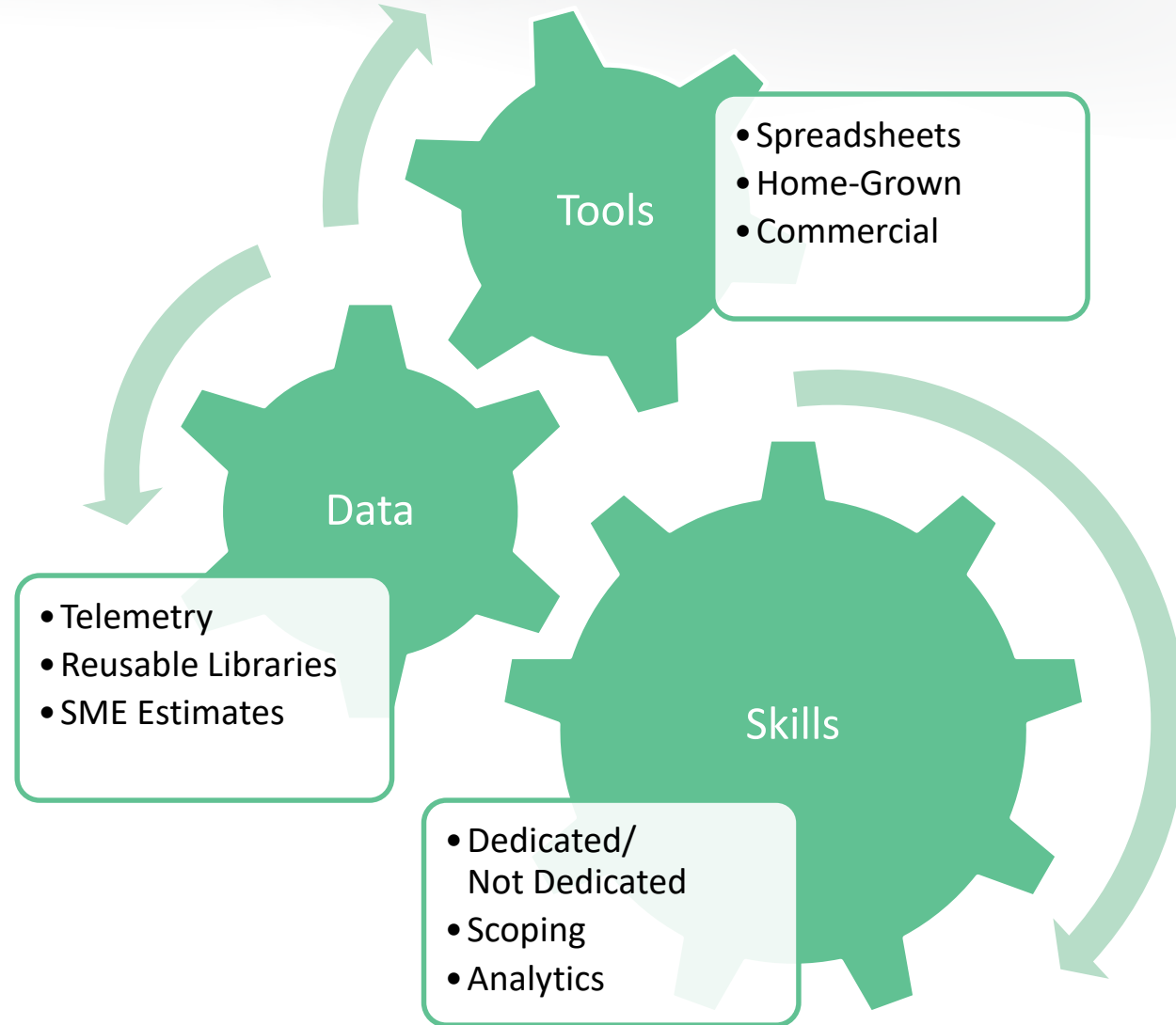


Compliance Requirements
The degree to which an organization is subject to meaningfully enforced external risk management expectations.

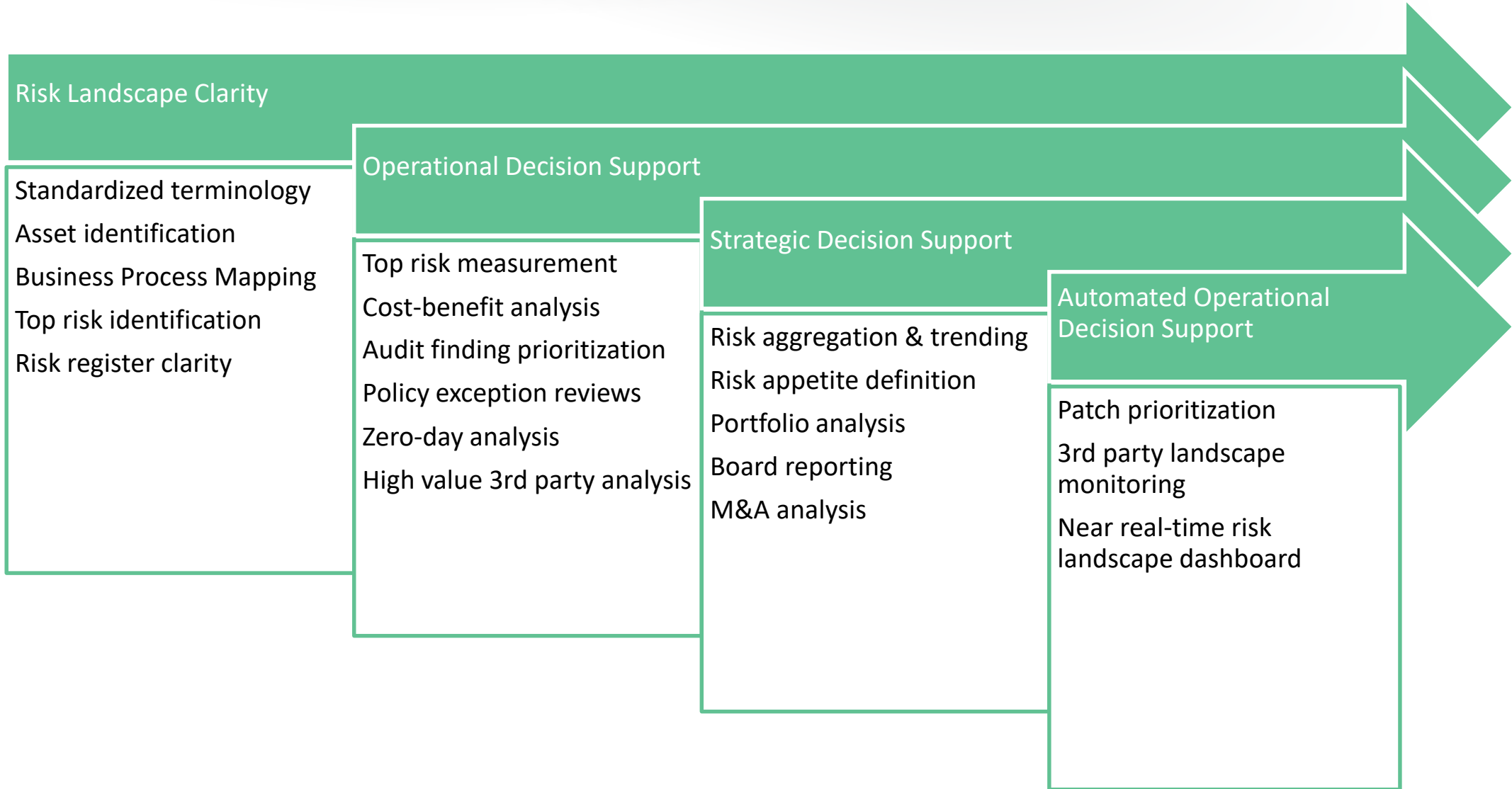
Organizational Resources
The probability that the organization has sufficient financial resources to meet its risk management needs and obligations given other organization imperatives.

Risk Landscape Intelligence
The probability that decision-makers are provided with the information needed to establish priorities and choose solutions, both at a strategic and operational level.

Risk Mgmt Maturity Resource Requirements



Four Dimensions of Risk Mgmt Maturity



Risk Management Maturity Evaluation

<p>2 RISK LANDSCAPE CLARITY</p> <ul style="list-style-type: none"> <input type="checkbox"/> Standardized terminology <input type="checkbox"/> Asset identification <input type="checkbox"/> Business Process Mapping <input type="checkbox"/> Top risk identification <input type="checkbox"/> Risk register clarity 	<p>3 OPERATIONAL DECISION SUPPORT</p> <ul style="list-style-type: none"> <input type="checkbox"/> Top risk measurement <input type="checkbox"/> Cost-benefit analysis <input type="checkbox"/> Audit finding prioritization <input type="checkbox"/> Policy exception reviews <input type="checkbox"/> Zero-day analysis <input type="checkbox"/> High value 3rd party analysis 	<p>4 STRATEGIC DECISION SUPPORT</p> <ul style="list-style-type: none"> <input type="checkbox"/> Risk aggregation & trending <input type="checkbox"/> Risk appetite definition <input type="checkbox"/> Portfolio analysis <input type="checkbox"/> Board reporting <input type="checkbox"/> M&A analysis 	<p>5 AUTOMATED OPERATIONAL DECISION SUPPORT</p> <ul style="list-style-type: none"> <input type="checkbox"/> Patch prioritization <input type="checkbox"/> 3rd party landscape monitoring <input type="checkbox"/> Near real-time risk landscape dashboard
--	--	--	---

<p>Skills</p> <ul style="list-style-type: none"> <input type="checkbox"/> Dedicated/Not Dedicated <input type="checkbox"/> Scoping <input type="checkbox"/> Analytics 	<p>Data</p> <ul style="list-style-type: none"> <input type="checkbox"/> Telemetry <input type="checkbox"/> Reusable Libraries <input type="checkbox"/> SME Estimates 	<p>Tools</p> <ul style="list-style-type: none"> <input type="checkbox"/> Spreadsheets <input type="checkbox"/> Home-Grown <input type="checkbox"/> Commercial
<p>1 RISK MGMT RESOURCES</p>		

RSA®Conference2020

Q & A (10 mins)

RSA®Conference2020

Group-Based Discussion (15 mins)

RSA®Conference2020

Group Summaries (10 mins)

Apply What You Have Learned Today

- Next week you should:
 - Validate maturity evaluation with your organization
- In the first three months following this presentation you should:
 - Develop near term plans to shore up resource requirements
- Within six months you should:
 - Improve risk landscape clarity and move into operational decision support